The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

DATE(S) ISSUED:
02/12/2013

SUBJECT:
Vulnerability in .NET Framework Could Allow Elevation of Privilege (MS13-015)

OVERVIEW:
A vulnerability has been discovered in the Microsoft .NET Framework which could allow an attacker to take complete control of an affected system. Microsoft.NET is a software framework for applications designed to run under Microsoft Windows. This vulnerability can be exploited if a user visits or is redirected to a malicious web page or runs a specially crafted Microsoft.NET application.

Successful exploitation of this vulnerability could allow an attacker to obtain complete control of the affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

SYSTEMS AFFECTED:
- Microsoft .NET Framework 2.0
- Microsoft .NET Framework 3.5 (except SP1)
- Microsoft .NET Framework 3.5.1
- Microsoft .NET Framework 4
- Microsoft .NET Framework 4.5 (except on Windows RT)

RISK:

Government:
- Large and medium government entities: **High**
- Small government entities: **High**

Businesses:
- Large and medium business entities: **High**
- Small business entities: **High**

Home users: High

DESCRIPTION:

An elevation of privilege vulnerability exists in the way that the .NET Framework elevates the permissions of a callback function when a particular Windows Forms object is created. Exploitation could occur if a user visits a specially crafted website that hosts malicious XBAP (Extensible Application Markup Language Browser Application) content using a web browser capable of instantiating XBAPs. Additionally, an attacker can exploit this issue by creating a specially crafted Windows .NET application to bypass Code AccessSecurity (CAS) restrictions.

An attacker who successfully exploited this vulnerability could take complete control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

RECOMMENDATIONS:

The following actions should be taken:

- Apply appropriate patches provided by Microsoft to vulnerable systems immediately after appropriate testing.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un trusted sources.
- Unless there is a business need to do otherwise, consider disabling XAML browser applications (XBAP) in Internet Explorer 6, 7, 8. By default, Internet Explorer 9 and Internet Explorer 10 prevent XAML, which is used by XBAPs

REFERENCES:

Microsoft:

http://technet.microsoft.com/en-us/security/bulletin/ms13-015

CVE:

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-0073

SecurityFocus:

http://www.securityfocus.com/bid/57847